Е. А. Береснева

# ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ В РОССИИ

Как только в Интернет пришел бизнес, а с ним и необходимость всегда точно определять, с кем имеешь дело, довольно широко стали использоваться технологии, позволяющие аутентифицировать субъектов Сети — как пользователей, так и серверы. Одна из них — электронная подпись (ЭП), стандарт которой (DSS) был выработан в 1991 г. Электронная подпись — это вставка в данные фрагмента инородной зашифрованной информации. Сама передаваемая информация при этом никак не защищается, т. е. остается открытой и доступной для ознакомления тем, через которых она передается (например, администраторам и инспекторам почтовых узлов связи). Инородная зашифрованная информация формируется с использованием двух методов: хэш-функции для подсчета контрольной суммы и для шифрования результатов с открытым ключом.

Фактически с 1990 г. в России на коммерческий рынок стали продвигаться так называемые технологии *электронной цифровой подписи* (ЭЦП). Системы ЭЦП позволяют создавать в электронных документах аналог собственноручной подписи. При этом речь не идет, например, о технологиях, позволяющих сохранять в электронном виде графическое изображение подписи. Механизмы ЭЦП существенно отличаются от простого анализа изображения и основаны на сложных математических задачах. Иными словами, подпись в электронном виде — это набор цифр, позволяющий не только идентифицировать лицо, сформировавшее эту подпись, но и обеспечить неизменность документа после подписания. Первым в России официально электронную подпись летом 1993 г. использовал Межбанковский финансовый дом.

В Соединенных Штатах закон об электронной подписи (E-SIGN Act) вступил в силу осенью 2000 г., и Билл Клинтон подписал его двумя способами — обычной шариковой ручкой и специальной карточкой со встроенным микропроцессором. Такие карточки и являются техническим средством, позволяющим ставить электронную подпись, но есть и другие варианты: обычный электронный пароль, интернет-планшет, видеоска-

нер, лазер для идентификации глаз или распознаватель голоса.

Гражданский кодекс РФ (ГК РФ) закрепил возможность использования ЭЦП, наряду с иными аналогами собственноручной подписи в электронном документообороте: «Использование при совершении сделок... цифровой подписи... допускается в случаях и порядке, предусмотренных законом, иными правовыми актами или соглашением сторон» (ГК РФ, ч. 1, ст. 160, п. 2); «Если стороны договорились заключить договор в определенной форме, он считается заключенным после придания ему условленной формы, хотя бы законом для договоров данного вида такая форма не требовалась» (ГК РФ, ч. 1, ст. 434, п. 1); «Договор в письменной форме может быть заключен... путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору» (ГК РФ, ч. 1, ст. 434, п. 2).

С момента принятия части первой ГК РФ в России сложилась богатая практика, в т. ч. судебная, по использованию систем ЭЦП в коммерческом секторе. Базой для упорядочения взаимоотношений сторон, использующих ЭЦП в бизнес-процессах, являлся так называемый *договор сторон*, или *договор участников системы с использованием ЭЦП*.

В системах документооборота государственных органов применение ЭЦП было ограничено, поскольку регулировать использование ЭЦП в этих системах договорным правом невозможно, т. е. сложилась ситуация, в которой принятие закона «О цифровой подписи» становилось необходимым в первую очередь для государства. Кроме того, Россия стремилась вступить во Всемирную торговую организацию (ВТО), а страны-члены ВТО уже имели аналогичные законы, позволяющие вести бизнес в киберпространстве не только на основе предварительно заключенного договора, но и на основе действующих законов. Теоретически принятие закона «О цифровой подписи» несло потенциальные выгоды также и потребителям услуг, позволяя им вступать в правоотношения без предварительного заключения договора в бумажном виде.

Основными разработчиками закона стали организации с серьезными межведомственными противоречиями — ЦБ РФ, Минсвязи РФ и ФАПСИ. С 1997 по 2001 г. было создано более 20 вариантов законопроекта. Результаты работы:

Из всех возможных систем цифровой подписи выбрана одна — электронная цифровая подпись.

Применение систем с использованием ЭЦП подлежит лицензированию, продукты — обязательной сертификации.

Введен ряд новых видов предпринимательской деятельности, подлежащих лицензированию.

Закон не соответствует рекомендациям ВТО. Системы ЭЦП, описанные в Законе об ЭЦП, заведомо несовместимы с международными стандартами.

После нескольких лет разработок закон «Об электронной цифровой подписи» был подписан президентом РФ 10 января 2002 г.

Цифровая подпись (ЦП) является частным случаем аналога собственноручной подписи (АСП). В свою очередь, электронная цифровая подпись является частным случаем цифровой подписи. На сегодняшний день используется большой набор различных АСП — биометрические, PIN-коды, факсимильные и т. д. В том числе широко используются системы цифровой подписи.

Технологии ЦП разнообразны и строго дифференцированы. Среди всех возможных технологий выбрана одна, четко определенная в законе и названная ЭЦП. Таким образом, в связи с принятием закона изменился только порядок применения электронной цифровой подписи — одного из аналогов собственноручной подписи.

Поскольку среди всех возможных аналогов собственноручной подписи закон регулирует применение ЭЦП, регулирование порядка применения иных АСП остается неизменным, а именно основывается на ГК РФ, предусматривающем заключение соглашения сторон. На этот факт прямо указывает пункт 2 статьи 1 закона «Об электронной цифровой подписи»: «Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи».

Дефиниция понятия ЭЦП приведена в законе «Об электронной цифровой подписи»: «Электронная цифровая подпись — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе».

Таким образом, электронная цифровая подпись неразрывно связывается с понятиями сертификата ключа, криптографического преобразования и электронного документа. Следовательно, к системам ЭЦП следует относить только системы подтверждения подлинности электронных документов с использованием сертификатов и основанных на криптографических преобразованиях. Кроме того, использование ЭЦП согласно закону возможно только для электронных документов. Закон не распростра-

няет свое действие на другие типы документов. Строгое определение электронного документа сегодня отсутствует.

В подготовленном законопроекте «Об электронном документе» указывается, какие именно реквизиты должны быть обязательны для электронного документа:

- обозначение и наименование документа;
- даты создания, утверждения и последнего изменения;
- сведения о создателях;
- сведения о защите электронного документа;
- сведения о средствах электронной цифровой подписи или средствах хэширования, необходимых для проверки электронной цифровой подписи или контрольной характеристики данного электронного документа;
- сведения о технических и программных средствах, необходимых для воспроизведения электронного документа;
- сведения о составе электронного документа.

Понятие криптографического преобразования в законе и иных нормативных документах, имеющих юридическую силу, отсутствует.

С другой стороны, определение понятия средств криптографической защиты информации (СКЗИ) и шифровальных средств имеется в ведомственных документах ФАПСИ. В связи с этим средства цифровой подписи (устоявшийся международный термин — *digital signature*), построенные без использования системы сертификатов, а именно такие системы в большинстве используют российские потребители, не являются системами ЭЦП с точки зрения определения закона.

Более того, системы с использованием сертификатов, но без создания удостоверяющих центров, а также системы, в которых подписи зарегистрированы на юридическое лицо, с точки зрения рассматриваемого закона относятся к иным аналогам собственноручной подписи и законом не регулируются.

Также к системам ЭЦП не относятся системы, в которых аналоги собственноручной подписи, в т. ч. ЦП, используются для удостоверения данных, не являющихся электронными документами.

Технически ЭЦП представляет собой набор байтов, который является результатом работы программы генерации цифровой подписи. Она является аналогом физической подписи и обладает двумя основными свойствами: 1) воспроизводима только одним лицом, а подлинность ее может быть удостоверена многими; 2) неразрывно связана с конкретным документом, и только с ним. ЭЦП предназначена для обеспечения подлинности, целостности и авторства документов, обрабатываемых с помощью вычислительной техники. Она жестко увязывает в одно целое содержа-

ние документа и секретный ключ подписывающего и делает невозможным изменение документа без нарушения подлинности этой подписи.

Суть процедуры использования ЭЦП состоит в том, что каждый пользователь программного обеспечения имеет возможность изготовить пару индивидуальных ключей: секретного — для формирования цифрового аналога подписи под документом и парного с ним, открытого — для проверки достоверности цифровых подписей, вычисленных с помощью данного секретного ключа. С помощью открытого ключа пользователя можно гарантированно подтверждать подлинность и авторство электронных документов, что именно данная последовательность бит была передана и подписана обладателем секретного ключа, соответствующего открытому ключу проверки. Секретный ключ для электронной цифровой подписи может храниться в виде файла на дискете или на специальном устройстве — «таблетке» (*Touch-Memory*). Их называют *носителями секретного ключа.*

В алгоритмах электронной подписи и асимметричного шифрования используются секретный и открытый ключи. Причем секретный должен браться абсолютно случайно, — например, с датчика случайных чисел, а открытый — вычисляться из секретного таким образом, чтобы получить второй из первого было невозможно.

Как и любые криптографические алгоритмы с открытым ключом, ЭЦП удобны для распределения ключей «на лету», что особенно удобно для пользователей Интернета: вы можете послать свой открытый ключ любому адресату непосредственно перед отправкой ему подписанного вами сообщения или, что еще проще, разместить его на каком-либо ресурсе в Интернете.

Сейчас существует множество алгоритмов ЭЦП, например отечественный стандарт электронной подписи — ГОСТ Р34.10–94, который, как и стандарт симметричного шифрования ГОСТ 28147–89, был обязателен для применения в государственных организациях России и обменивающихся с ними конфиденциальной информацией коммерческих организациях; новый отечественный стандарт ГОСТ Р34.10–2001; различные общеизвестные алгоритмы ЭЦП, например RSA (*Rivest – Shamir – Adleman*), Эль-Гамаля, DSA (*Digital Signature Algorithm*).

Поскольку шифрование защищает сообщения от ознакомления, а ЭЦП — от подмены (две основные угрозы информации в Интернете), то было бы логично для обеспечения более полной безопасности совместно применять ЭЦП и комбинированное шифрование.

Международный опыт, прежде всего Организации Объединенных Наций и Европейского экономического сообщества, выделяет два основных направления решения проблем правового регулирования электрон-

ного документооборота — принятие нормативных правовых актов 1) об электронной торговле и 2) электронной подписи.

Законы об электронной подписи приняли многие страны мира — Австрия, Беларусь, Великобритания, Индия, Ирландия, Республика Корея, Россия, Литва, Польша, Таиланд, Финляндия, Франция, Филиппины, Эстония.

Несмотря на ряд серьезных противоречий, Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» создает необходимую правовую основу для регулирования отношений, возникающих при электронном документообороте в государственных корпоративных информационных системах и системах общего пользования, в том числе и в коммерческой среде.